[EDISI SPESIAL]

ROOTMAGZ

MAJALAH KOMPUTER DIGITAL

EDISI SPESIAL VIRUS 02/2015

Plus Glosarium!

Majalah Ini Dilengkapi Kamus Istilah untuk Memudahkan Anda Belajar Komputer

Mengenal Virus

Ketahui Klasifikasi Malware di PC Windows

EDISI SPESIAL VIRUS +SOLUSI

Mengenal Solusi Virus

Menggunakan Linux Salah Satunya!

Mengenal Antivirus

Ketahui Bagaimana Antivirus Diciptakan, Jangan Ada Salah Paham

Mengenal Virus Komputer

Ade Malsasa Akbar <teknoloid@gmail.com>

Tahu Sumber Masalah, Tahu Pemecahannya

Apa itu virus komputer? Banyak orang tahu tetapi tidak tahu apa hakikat virus itu. Ketika komputer (Windows) terjangkit virus, orang awam biasanya pasrah kepada tukang servis untuk instal ulang. Jika virus sering menyerang, berapa kali servis dilakukan? Berapa biaya yang habis? Cara yang lebih murah adalah menggunakan antivirus. Hal ini menimbulkan masalah lagi. Ada satu keadaan ketika antivirus menghapus **berkas**-berkas pengguna. Masalah pun tambah runyam. Inti permasalahan adalah pengetahuan. Pengguna awam (pengguna Windows) biasanya tidak mengenal apa itu virus, bagaimana pencegahannya, dan bagaimana penanganannya. Maka kami memperkenalkan hal itu kepada pembaca dalam tulisan ini dengan bahasa yang mudah.

Peristilahan

Istilah "virus" terus menerus digunakan sebetulnya kurang tepat. Orang biasanya menyebut virus, karena sebelumnya sudah mengenal antivirus. Masalah yang dihadapi pengguna awam adalah serangan oleh program jahat. Istilah yang umum mencakup semua jenis program jahat itu adalah malware (malicious software = program berpenyakit). Istilah ini seperti istilah sepeda motor, yang termasuk di dalamnya Suzuki, Honda, Yamaha, dan sebagainya. Istilah malware melingkupi virus, worm, trojan horse, ransomware, spyware, adware, dan botnet. Penyebutan ini bukan pembatasan karena masih banyak klasifikasi malware lain. Untuk menyederhanakan, kami sampaikan beberapa ini yang terpenting.

Virus

Virus komputer (computer virus) adalah program yang, ketika di**eksekusi**, mampu menduplikat dirinya sendiri dan menginjeksikan dirinya itu ke dalam program lain. Ketika suatu program diinjeksi oleh virus, maka kita menyebut program itu "terinfeksi". Ketika program terinfeksi dijalankan, maka otomatis virus ikut berjalan pula. Ketika mereka berdua berjalan bersama-sama di memori, virus biasanya beraksi entah itu menduplikat dirinya kembali atau menginjeksi kembali atau bahkan hal-hal yang sifatnya merusak di sistem Windows pengguna. Klasifikasi virus bisa diterapkan berdasarkan tipe target entah dia menyerang **binary executable** alias program (formatnya .msi, .exe, .com), berkas data (seperti .doc, .ppt, .xls), atau boot sector pada hard disk. Contoh virus yang sangat terkenal di dunia adalah W32/Simile (dilaporkan muncul tahun 2002), virus yang mampu menulis ulang dirinya sendiri (metamorphism) sehingga begitu sulit dikenali pihak peneliti atau antivirus.

Worm

Worm (cacing) adalah program yang, ketika dieksekusi, mampu menduplikat dirinya sendiri dengan tujuan menyebar melalui jaringan atau **media penyimpanan**. Berbeda dengan virus, worm tidak menginjeksikan dirinya ke program lain. Worm punya dampak negatif yang besar sekali di antaranya sulit dibersihkan karena terduplikasi ke semua komputer di jaringan serta ke semua HD atau FD. Selain itu, worm juga dapat memakan bandwidth internet di jaringan, berkebalikan dengan virus yang selalu merusak berkas-berkas atau program-program Windows. Tidak hanya itu, beberapa tipe worm juga bisa menghapus berkas pengguna, mengirim email, atau mem-password (mengenkripsi) data pengguna. Contoh worm yang paling terkenal adalah Conficker, yang menginfeksi sekitar 15 juta komputer Windows di dunia termasuk jaringan komputer angkatan laut Prancis menurut Wikipedia.

Trojan Horse

Trojan horse (kuda troya) adalah program kendali jarak jauh. Jika sebuah trojan memasuki komputer pengguna, pemilik trojan (si penjahat) bisa mengendalikan komputer tersebut walau dari negara lain sekalipun asal ada internet. Kendalinya bisa berupa shut down, restart, hapus berkas, masukkan berkas (termasuk virus), format **hard disk**, memonitor kegiatan pengguna, dan lain-lain. Mitologi perang Troya ketika kerajaan A menghadiahkan kuda kayu raksasa ke kerajaan B, kemudian B menerima lalu ternyata isi kuda itu pasukan kerajaan A dan kerajaan lawan ini kalah karena itu. Itulah asal penamaan Trojan Horse (Trojan). Prinsipnya sama. Contoh trojan yang sangat terkenal misalnya BackOrifice2000 (BO2000). Trojan ini tersedia gratis untuk Windows sehingga sangat berbahaya jika digunakan selain orang yang benar.

Ransomware

Ransomware (ransom + software = program penyandera) adalah program yang mem-password (mengenkripsi) komputer pengguna dan meminta tebusan uang. Enkripsi yang dipakai biasanya 1024-bit ke atas (tidak bisa dijebol) yang melazimkan orang membayar demi kembalinya data. Itu pun belum tentu benar karena namanya pembuat malware adalah penjahat yang tidak bisa dipercaya. Ransomware adalah salah satu jenis trojan tetapi masuk jadi kategori sendiri saking besar dampak negatifnya. Ransomware mulai marak di Indonesia dan kami melihat banyak pengguna awam terkena dan semuanya tidak bisa berbuat apa-apa. Ransomware mungkin dihapus, tetapi data yang terenkripsi tidak bisa dikembalikan. Apalagi jika yang dienkripsi satu HDD. Contoh ransomware adalah Cryptolocker yang hanya menyerang Windows.

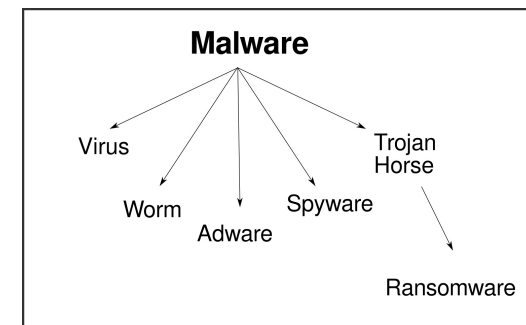



Diagram Klasifikasi Malware

Spyware

Spyware adalah program spy, mata-mata. Sekali spyware masuk ke komputer pengguna, aktivitas apa saja bisa diketahui penjahat pemilik spyware. Pengguna browsing situs tertentu, memiliki password tertentu, memutar video tertentu, membuka dokumen tertentu, semua itu bisa diketahui si penjahat. Kenapa? Karena itu tugas spyware. Dia akan melaporkan apa pun yang diawasinya kepada pemiliknya melalui internet. Dampak spyware

GLOSARIUM

Berkas
Terjemahan Indonesia untuk istilah "file". Berkas adalah istilah umum untuk menyebut satu data digital tertentu di komputer. Dokumen DOC berkas, audio MP3 berkas, TXT juga berkas.

Eksekusi
Menjalankan program. Istilah eksekusi (to execute, execution) digunakan pada tahap kegiatan untuk menjalankan (to run, running) sebuah program. Klik dua kali pada EXE di Windows disebut eksekusi dan perintah ./ di Linux juga disebut eksekusi. Setiap malware pada dasarnya tidak akan menyerang kecuali dieksekusi sendiri oleh pengguna sadar ataupun tidak.

Binary Executable
Eksekutabel biner, berkas biner (berisi kode 0 dan 1) yang bisa dieksekusi. EXE di Windows tergolong binary executable. DEB di Linux tergolong juga binary executable.

Media Penyimpanan
Storage media. Istilah umum untuk menyebut penyimpanan digital yang bisa menyimpan data permanen. Contoh media penyimpanan adalah hard disk.

Source Code
Kode sumber. Kode resep asli dari sebuah program. Setiap program di muka bumi diciptakan dari source code.

Tahukah Anda?

RPM (Red Hat Package Manager) adalah nama format eksekutabel biner untuk Red Hat Linux dan keturunannya (Fedora, CentOS, IGOS Nusantara, dll.). Di Windows, RPM itu seperti format EXE atau MSI. Logo di samping adalah logo resmi RPM.

ReactOS adalah sistem operasi free yang dibuat untuk kompatibel dengan Windows secara binary. ReactOS diciptakan seperti Linux diciptakan, dikembangkan dari luar tanpa mengambil **source code** dari Windows. Hasilnya, ReactOS dapat menjalankan EXE dan driver Windows secara native. ReactOS lahir tahun 1998 (17 tahun lalu).

GLOSARIUM

CPU
Central Processing Unit. Istilah untuk menyebut prosesor komputer. CPU bertugas memroses data. Letak fisik CPU ada di tengah atas mainboard di dalam box case komputer. CPU memiliki kecepatan proses, memori internal (disebut cache), ALU (Arithmethic Logical Unit), dan lain-lain.

Browsing
Menjelajah. Istilah untuk menyebut kegiatan membaca suatu website pada web browser.

Network
Jaringan komputer. Kumpulan komputer yang dihubungkan oleh media penghubung dengan aturan-aturan tertentu. Di dalam network, pasti terdapat protokol, topologi, mekanisme routing, konfigurasi jaringan, dan penghubung (kabel, nirkabel, dsb.).

Spam
Email sampah. Istilah spam pada awalnya ditujukan untuk email sampah. Kini istilah spam meluas, bisa dipakai menyebut website yang tidak berguna, posting iklan tidak berguna, entri pencarian yang tidak relevan, dan sebagainya.

bisa mulai dari bypass (pembelokan) browsing ke alamat tertentu yang tidak diinginkan, bom iklan, beban **CPU** yang abnormal, pencurian bandwidth internet tanpa izin, dan lain sebagainya. Spyware tidak menyebar dengan cara virus atau worm, tapi dengan mengeksploitasi kelemahan sistem Windows pengguna. Sejumlah spyware masuk dari web ketika pengguna sedang **browsing**. Spyware dan pembuatnya adalah kriminal dan dapat dijatuhi sanksi karena kejahatannya. Contoh spyware yang terkenal misalnya DollarRevenue yang pembuatnya dituntut denda 1.000.000 Euro (di atas 14 miliar rupiah, kurs September 2015) karena menginfeksi 22.000.000 komputer di Eropa.

Adware
Adware adalah program iklan. Sekali adware masuk komputer pengguna, dia akan mengebomnya dengan iklan. Tujuan pembuat adware hanyalah uang dari iklan. Dampak adware di antaranya munculnya jendela pop-up (jendela tiba-tiba) yang banyak yang berisi iklan, sebagiannya tidak bisa ditutup.

Botnet
Botnet (robot + **network** = jaringan robot) adalah malware yang memasuki komputer pengguna dengan jalan apa pun, mengubahnya menjadi zombie, dan melakukan suatu tindakan yang tidak diketahui pengguna. Botnet biasanya dibuat untuk menginfeksi banyak komputer dengan tujuan DDOS (distributed denial of service) yakni menyerang bersama-sama terhadap suatu layanan di internet. Selain itu, komputer zombie yang sudah diinfeksi oleh botnet, jika besar jumlahnya, bisa juga digunakan untuk mengirim spam kepada komputer-komputer lain. Selain itu pula, masih banyak kegiatan jahat lain yang bisa dilakukan karena jumlah zombie yang besar tersebut. Sekali lagi, semua kegiatan jahat itu tidak diketahui oleh pemilik komputernya. Maka jangan heran jika mungkin akun email Anda pernah dimasuki **spam**. Botnet juga bisa berbentuk akun Facebook yang menyebarkan spam atau gambar asusila secara otomatis kepada akun-akun lain atau kepada grup-grup atau menarik masuk grup temannya yang juga botnet. Botnet dengan jumlahnya yang banyak, bisa digunakan penjahatnya untuk melakukan klik secara massal kepada iklan di **website** miliknya yang ujung-ujungnya uang baginya. Contoh botnet terkenal baru-baru ini adalah Ramnit yang dilaporkan menginfeksi 3.000.000 komputer.

Mengapa Membuat Malware?
Ada dua alasan konkret mengapa orang membuat malware. Satu, pertama kalinya, untuk penelitian ilmiah. Satu cabang ilmu komputer adalah software engineering (rekayasa perangkat lunak) yang mempelajari penciptaan perangkat lunak. Termasuk di sana bagaimana menciptakan perangkat lunak yang mampu memodifikasi atau mereplikasi dirinya sendiri. Waktu berlalu, muncul penelitian lain yakni bagaimana menangani perangkat lunak berpenyakit (malware) tersebut dengan perangkat lunak pula (antimalware, antivirus). Dua, untuk uang. Ransomware adalah satu bukti konkret. Pembuat ransomware bisa kaya raya dalam sekejap karena menyandera komputer orang. Tentu hal ini kejahatan sekaligus tindakan kriminal. Selain itu, program seperti trojan horse bisa digunakan penjahat untuk mencuri password pengguna. Termasuk pula mencuri data kartu kredit maupun data rekening bank.

Di luar dua alasan konkret di atas, ada alasan-alasan lain. Di antaranya alasan dendam, alasan protes, alasan pelampiasan perasaan, maupun alasan just for fun (karena pemrograman/rekayasa perangkat lunak memang menyenangkan). Ada juga alasan seni karena sejumlah malware menyertakan karya seni visual atau sastra di dalam serangan-serangannya. Apa pun alasannya, pembaca harus kritis terhadapnya. Jangan merusak, mengambil, atau mengalihkan, hak orang lain tanpa izin. Jangan login ke komputer orang tanpa izin.

Mengapa Sulit Menangkap Pembuat Malware?
Kejahatan malware bukan kejahatan fisik. Pencopet di terminal bisa ditangkap karena perbuatannya fisik sehingga bisa ditindak langsung secara fisik. Pencopet di dunia software komputer tidak demikian. Bagaimana Anda tahu virus A.A dibuat oleh si fulan dari negara allan? Mengidentifikasi virus itu sendiri sudah satu kesulitan, mengidentifikasi pembuatnya juga satu kesulitan, mengidentifikasi lokasi geografis pelaku juga satu kesulitan yang lain. Semua pembuat malware tidak terlalu bodoh untuk meletakkan nama, alamat, KTP, dan nomor telepon aslinya di dalam malware-nya.

Bagaimana Malware Menyerang PC?
Yang umum dirasakan, malware menyerang PC Windows. Hal ini diakibatkan banyak faktor. Di antaranya, malware memanfaatkan celah keamanan (vulnerability) Windows. Selain itu, ada teknik psikologis yang bernama social engineering (rekayasa sosial) yang bisa menipu mata pengguna dan membuatnya mengeksekusi malware tanpa paksaan dalam ketidaksadaran. Misalnya menyamarkan nama berkas tukul-ndeso.exe menjadi tukul-ndeso.jpeg.exe. (ada tambahan JPEG). Pengguna Windows awam seringkali terkecoh dengan trik simpel macam itu. Di luar itu, kebiasaan tidak aman sering dilakukan pengguna Windows pula. Misalnya menginstal perangkat lunak bajakan, sembarangan mengunjungi web, sembarangan memakai flash disk tanpa kepastian, dan sebagainya. Demikian sekilas perkenalan dengan malware. •

Tahukah Anda?

Archlinux adalah salah satu OS Linux yang memegang prinsip kesederhanaan desain. Arch ditujukan untuk pengguna ahli, sistem rilisnya rolling release, dan merupakan distro Linux yang memiliki koleksi software paling lengkap. Logo di samping adalah logo Archlinux.

Referensi

- https://en.wikipedia.org/wiki/Spyware
- https://en.wikipedia.org/wiki/Computer_virus
- https://en.wikipedia.org/wiki/Heuristic_(computer_science)
- https://en.wikipedia.org/wiki/Adware
- https://en.wikipedia.org/wiki/Botnet
- https://en.wikipedia.org/wiki/Malware
- https://en.wikipedia.org/wiki/Ramnit
- https://en.wikipedia.org/wiki/Ransomware
- https://en.wikipedia.org/wiki/Trojan_horse_(computing)

Mengenal Antivirus

Bikin Antivirus Itu Susah, Bung!

Ade Malsasa Akbar <teknoloid@gmail.com>

Semua orang pasti menggunakan antivirus di Windows-nya. Ini tindakan pencegahan terhadap serangan dari luar yang seringkali terjadi. Namun belum tentu orang tahu apa antivirus itu dan bagaimana bisa dia ada. Sebuah pertanyaan yang butuh penjelasan panjang. Kami hadirkan singkat di sini untuk pembaca.

Peristilahan
Istilah antivirus telah diterima sebagai budaya yang tidak dipertanyakan lagi. Sebenarnya istilah ini terlalu spesifik. Istilah yang lebih tepat adalah antimalware. Karena dewasa ini tugas antivirus tidak cuma membersihkan virus, tapi juga malware yang lain. Namun tidak mengapa tetap dipakai istilah antivirus di sini.

Apa Antivirus Itu?
Antivirus adalah program komputer yang diciptakan untuk mendeteksi, mencegah, dan mengobati dampak dari virus dan malware. Perbuatan yang dilakukan oleh antivirus antara lain

Tahukah Anda?

MATE adalah desktop environment yang dikembangkan dari GNOME 2. Pengembangan MATE dikarenakan proyek GNOME 2 dihentikan oleh pengembang aslinya padahal masyarakat masih menyukai GNOME 2. Maka bisa dikatakan MATE = GNOME 2 yang masih hidup. Tampilan MATE sama persis dengan GNOME 2. Logo di samping adalah logo MATE.

GLOSARIUM

Memori
Jenis Istilah untuk menyebut penyimpanan sementara di komputer. Memori bisa dibagi atas (RAM Random Access Memory) dan ROM (Read Only Memory). Namun dalam perkembangannya sering dipakai untuk menyebut RAM saja.

Proses
Process. Jika sebuah program dieksekusi, dia akan dipindahkan ke memori untuk di-process. Saat itulah program tersebut disebut process. Sebuah process memiliki PID (Process Identifier) yakni tanda pengenal proses yang biasanya berupa angka.

Disassembling
Proses mengubah kembali program binary menjadi source code bahasa assembly. Disassembling dilakukan dengan bantuan program disassembler.

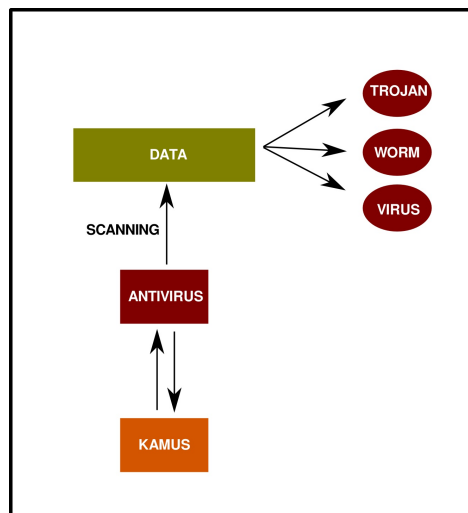
Debugging
Proses menemukan bug (kesalahan pemrograman) pada sebuah program. Dengan debugging, diketahui mengapa suatu program berperilaku tertentu. Debugging merupakan salah satu dari tahap-tahap pemrograman perangkat lunak. Debugging dilakukan dengan bantuan program debugger.

memory monitoring, **file scanning**, **heuristic scanning**, dan **quarantining**. Tugas antivirus itu berat, tapi masih lebih berat tugas pembuat antivirus. Di dalam dunia perantivirusan, kita mengenal heuristic engine dan signature. Kita akan bahas semua itu secara umum.

Memory Monitoring

Dilihat dari klasifikasinya, malware banyak yang punya sifat resident (menetap). Sekali malware dieksekusi, ia resident di **memori** sebagai program yang berjalan (process). Termasuk dalam hal ini, virus yang menyebar dari flash disk dan menginfeksi komputer yang mengakses flash disk itu. Sekali menginfeksi, dia akan langsung resident di memori. Memory monitoring adalah tugas antivirus untuk terus menerus bersiaga di memori. Jika tidak bersiaga, ketika ada malware yang resident, maka Windows akan terserang dan saat itu sudah terlambat. Maka dari itu umumnya antivirus selalu menyala bahkan ketika Windows Anda start. Beberapa antivirus memberi nama lain teknik ini, misalnya real-time monitor (RTM) di PCMAV.

File Scanning

Pemindaian berkas. Fitur paling standar di semua antivirus. Antivirus memeriksa satu atau seluruh berkas agar diketahui mengandung malware atau tidak. Jika mengandung malware, maka dilakukan tindakan selanjutnya. Misalnya dihapus atau dibersihkan (jika mungkin). Jika tidak ada cara, maka dikarantina (quarantine, vault).

Pada diagram di atas, diperlihatkan cara antivirus memindai. Cara ini memanfaatkan signature/definition yang di diagram disebut kamus. Ya, signature sebenarnya adalah kamus yang dibuat oleh pembuat antivirus berisi daftar kata (daftar malware) dan artinya (metode penanganannya). Antivirus ketika memindai, membandingkan data dengan kamus. Jika cocok, maka ditandai sebagai malware, dan biasanya ditayangkan kepada pengguna ini virus A, ini worm B, dan sebagainya. Lalu berdasarkan kamus (signature), antivirus bisa mengambil tindakan tertentu. Misalnya mencabut tubuh virus dari berkas, menghentikan **proses** worm di memori, dan sebagainya.

Signature

Signature adalah kamus virus. Signature biasa disebut juga definition. Signature inilah yang sebenarnya di-update ketika antivirus meminta update. Signature bisa disebut obat juga, yang diramu oleh dokter-dokter atau ahli farmasi yang disebut pembuat antivirus. Pembuatan signature sangat berat, karena prosesnya banyak dan panjang. Mulai dari pengambilan sampel malware, analisis (**disassembling**, **debugging**, decrypting, dsb.), sampai pada penanganan yang kemudian ditulis ke dalam kamus signature tersebut. Signature dibuat setiap hari, bahkan ada vendor yang update sehari dua kali, itu pun antivirusnya gratis (dan kadang masih juga dibajak). Sebelum signature dipublikasikan, si pembuat antivirus harus berhasil dulu mengalahkan malware tersebut di komputernya sendiri. Bagaimana caranya sementara antivirusnya saja belum ada? Bayangkan betapa sulit dan banyaknya kerjaan membuat satu signature saja. Apalagi setiap hari. Seharusnya layak pembuat antivirus disebut pahlawan tanpa tanda jasa bagi pengguna Windows.

Heuristic

Heuristic (bersifat mencari) adalah fasilitas standar antivirus untuk menemukan kode-kode berbahaya di dalam sebuah berkas tanpa kamus. Heuristic adalah satu jenis kecerdasan buatan yang dimasukkan ke dalam antivirus untuk mengenali malware baru tanpa perlu adanya kamus dahulu. Ya, antivirus bisa berpikir sendiri dan namanya adalah heuristic. Cara kerjanya pada umumnya adalah sengaja menjalankan malware tertentu di dalam suatu lingkungan virtual dan menganalisisnya. Bisa juga dengan sengaja memindai satu berkas dan membaca seluruh kodenya. Semua antivirus besar macam AVG, Avira AntiVir, Avast!, PCMAV, memiliki fasilitas ini. Heuristic di dalam suatu antivirus dikerjakan oleh komponen yang disebut heuristic engine (mesin heuristik).

Quarantine

Quantine (karantina) atau disebut juga Vault atau Chest adalah fasilitas isolasi kepada berkas yang dicurigai berbahaya. Ringkasnya, virus bisa disekap di dalam quarantine. Hal ini dilakukan dengan membuat suatu folder tertentu di sistem Windows dan memblokir di dalam folder itu ke luar. Segala program berbahaya di dalamnya tidak akan berkutik.

Contoh Antivirus

Secara wilayah, kita bisa membagi antivirus menjadi dua. Satu, internasional. Tergolong kategori ini Avira Antivir, Grisoft AVG, Avast!, BitDefender Kaspersky Antivirus, Symantec Norton Antivirus, Panda Antivirus, Comodo Antivirus, dan lain-lain. Dua, lokal. Tergolong kategori ini PC Media Antivirus (PCMAV), Ansav, dan Smadav. Secara fitur, kita bisa kategorikan berdasarkan tingkat kelengkapannya. Ada antivirus khusus untuk salah satu malware saja, ada antivirus yang menyeluruh untuk segala jenis malware.

Sekian perkenalan dasar antivirus.•

Tahukah Anda?

Red Hat Inc. adalah perusahaan yang mengembangkan Red Hat Enterprise Linux dan segala bisnis yang menyertainya. Logo Red Hat (Topi Merah) adalah seperti di samping.

Mengapa Antivirus Berbeda Deteksi?

Jangan Salah Paham

Ade Malsasa Akbar <teknoloid@gmail.com>

Kadang satu antivirus mendeteksi satu berkas sebagai virus, sedang antivirus lain tidak bereaksi apa-apa. Kadang satu antivirus mampu mencabut virus dari berkas-berkas yang terinfeksi, kadang antivirus lain tidak mampu, kadang juga ada antivirus menghapus total semua berkas milik pengguna. Pembaca bisa membuktikannya sendiri. Namun hal ini sering disalahpahami pengguna awam dan menghukumi suatu antivirus jelek berdasarkan itu. Perlu hal ini kita perjelas agar tidak ada salah paham.

Pada artikel sebelumnya, dijelaskan bagaimana secara umum antivirus dan signature-nya diciptakan. Dari situlah terdapat

Tahukah Anda?

Wikipedia adalah situs artikel-artikel ilmu pengetahuan yang bisa diedit oleh siapa saja. Wikipedia tersedia dalam semua bahasa di dunia dan seluruh cabang ilmu pengetahuan yang ada. Wikipedia merupakan salah situs paling banyak dikunjungi karena kontennya. Wikipedia dibuat dari perangkat lunak free software MediaWiki. Logo Wikipedia seperti di samping.

perbedaan dari satu antivirus ke yang lain. Selain itu, terdapat perbedaan dari virus itu sendiri. Kadang ada virus yang menempel di bagian awal berkas, ada yang menempel di bagian akhir berkas. Ada juga virus yang menghapus sebagian tubuh berkas dan memasukkan salinan virus ke dalam bagian yang dihapus itu. Berkas seakan-akan utuh, tapi sebagiannya sudah hilang dan diganti dengan virus. Itulah sekilas perilaku-perilaku virus yang umum. Ini baru virus. Belum malware yang lain.

Pencabutan
Suatu antivirus bisa mencabut virus-virus dari berkas-berkas Anda jika tipe virusnya sebatas menempel di awal atau di akhir. Antivirus bisa membaca bagian mana yang berkas, bagian mana yang virus. Amputasi dilakukan pada bagian virusnya, bagian asli berkasnya tetap.

Penyembuhan
Healing atau curing, bisa dilakukan jika virus bisa dikenali berdasarkan signature. Tentu bisa healing itu karena si pembuat antivirus membuat fungsi healing terhadap virus tersebut.

Penghapusan
Suatu antivirus memutuskan menghapus suatu berkas, bisa jadi karena virusnya adalah virus yang merusak berkas (virus penghancur). Virus tipe ini akan menghapus sebagian tubuh berkas dan meletakkan salinan dirinya ke dalam bagian yang kosong itu. Dari luar, kita melihat berkas utuh-utuh saja. Namun ternyata sudah rusak plus sudah tercampur virus. Kondisi seperti ini tidak bisa diamputasi tetapi harus dihilangkan beserta berkasnya. Kalaupun bisa virusnya diamputasi, sejak awal berkas sudah rusak dan tidak akan bisa digunakan. Maka perlu dimaklumi adanya tipe virus penghancur macam ini dan mengapa antivirus harus menghapusnya.

Bisa Berbeda!
Dari hal-hal di atas, kita kembali kepada signature. Pembuat antivirus satu dengan yang lain berbeda. Maka ada kemungkinan beda jumlah kamus. Bisa juga beda teknik penyembuhan. Bisa saja semua antivirus internasional memiliki kamus untuk Conficker, tapi belum tentu antivirus internasional punya kamus untuk virus lokal Yuyun.Cantik. Kenapa? Karena virus Yuyun.Cantik beredar di Indonesia saja. Sedangkan Conficker adalah worm internasional, wajar antivirus internasional tahu.

Lepas dari semua itu, cara seseorang memasak soto beda dengan orang lain. Sama juga dengan pembuat-pembuat antivirus. Bisa saja semua antivirus punya signature untuk Conficker. Tapi masing-masing signature punya cara sendiri untuk menyembuhkannya. Perbedaan itu bisa jadi dari urutan-urutan logikanya (**algoritma**) apa dulu yang dilakukan, bisa jadi pula kelengkapannya. Maka dari sini dimaklumi apabila terjadi penyembuhan oleh antivirus satu lebih baik dan lebih tuntas dari antivirus lain. Maka diketahui mengapa antivirus berbeda deteksi dengan antivirus lain.•

GLOSARIUM

Algoritma
Urut-urutan logika dalam pemrograman. Setiap perangkat lunak dibuat dengan algoritma tertentu, baik sedikit ataupun banyak. Menguasai algoritma juga syarat seseorang mempelajari pemrograman.

Flash Disk
Sebutan ringkas untuk USB Flash Disk atau USB Flash Drive. Media penyimpanan berukuran kecil, berantarmuka USB, yang menggunakan memori flash.

Celah Keamanan
Segala macam kekurangan teknis suatu perangkat lunak atau suatu sistem yang memungkinkan masuknya ancaman (malware, buffer overflow, buffer underrun, dsb.).

Software
Perangkat lunak. Suatu kumpulan instruksi yang dimengerti komputer yang mengerjakan tugas tertentu. Contoh software adalah Libreoffice.

Unggahan
Unggah = upload, unggahan = yang di-upload. Data yang diunggah, dipindahkan dari komputer lokal ke komputer remote.

Solusi Permasalahan Virus Windows

Anda Tidak Sendirian

Ade Malsasa Akbar <teknoloid@gmail.com>

Setelah bahaya dan kesulitan, perlu disebut solusi. Di dua pervirusan Windows, ada beberapa solusi teoretis dan praktis. Berikut kami tuliskan.

Security Awareness
Pengguna harus sadar keamanan. Punya sikap-sikap dasar keamanan. Misalnya, tidak sembarangan memberi hak akses kepada pihak lain. Sikap lain yang penting juga tidak sembarangan menggunakan disket, CD, hard disk, atau **flask disk**. Sikap yang juga penting adalah tidak sembarangan mengunjungi website. Banyak website berbahaya yang memanfaatkan **celah keamanan** Windows untuk memasukkan spyware. Sikap yang tak kalah penting adalah tidak menggunakan **software** bajakan, tidak mengunduhnya. Seringkali pembajak menyertakan trojan horse di dalam **unggahan** software bajakannya. Intinya, miliki kesadaran bahwa keamanan itu penting dan harus diutamakan.

Menggunakan Antivirus
Pilihlah antivirus yang bagus. Jika tidak bisa memilih, belilah antivirus berbayar yang bergaransi. Baca perbandingan kualitas antivirus di situs http://av-comparatives.org. Jangan sembarang menuruti rekomendasi orang di jalan yang Anda tidak tahu, karena ujungnya bisa jadi Anda kesal tidak sesuai rekomendasi dengan kenyataannya.

Belajar
Jika pembaca menggunakan Windows, antivirus sesungguhnya adalah brainware. Tanpa brain, antivirus pun tak bermakna. Saat penulis belajar pervirusan Windows, itu berguna sekali. Maka penulis rekomendasikan para pembaca untuk juga belajar. Di antara start yang mudah untuk pemula:

- antivirusworld.com
- virus.wikidot.com
- virusindonesia.com
- viruslokal.com

Menggunakan Linux
Satu solusi yang sangat praktis adalah menggunakan Linux di PC. Sudah banyak perusahaan yang migrasi (total ataupun parsial) dari Windows ke Linux karena masalah virus. Linux secara umum jauh lebih aman dari Windows. Virus (malware) Windows tidak akan bisa berjalan di Linux. Dan di Linux sendiri jumlah virus teramat sedikit dibandingkan Windows. Secara kenyataan, pembaca pun bisa bertanya kepada pengguna Linux di sekitar apakah mereka pernah terkena virus. Jawabannya bisa ditebak: tidak.

Menggunakan Linux tidak harus total. Anda bisa dualboot dengan Windows (1 komputer 2 OS). Anda juga bisa hanya sebatas live cd (OS Linux bisa digunakan tanpa diinstal). Banyak pilihan di Linux. Semua terserah Anda.

Metode penggunaan Linux bisa jadi secara total (digunakan layaknya menggunakan Windows sehari-hari) atau parsial. Parsial di sini bisa jadi hanya menggunakan Linux untuk memeriksa flash disk yang dicurigai bervirus. Kami telah bertahun-tahun menggunakan cara ini dan hasilnya sangat efektif. Virus tidak akan berjalan, autorun tidak akan berguna, maka semua virus bisa langsung dihapus dengan Delete di Linux. Di Windows, menghapus virus tidak semudah itu. Jadi, Anda bisa dualboot Windows-Linux, dan hanya boot ke Linux untuk menghapus virus sebelum flash disk dipakai di Windows.

Kesimpulan
Antivirus memang salah satu solusi yang bagus. Namun antivirus terbaik adalah brainware. Tanpa security awareness, memakai 1000 antivirus akan percuma saja. Solusi eksternal yang sangat bisa dipertimbangkan adalah menggunakan Linux.•

Tahukah Anda?

slackware
linux

Slackware adalah OS Linux tertua yang masih aktif dikembangkan sampai sekarang. Slackware berprinsip sederhana dalam desain. Slackware ditujukan untuk pengguna menengah ke atas. Logo Slackware seperti di samping.

Tahukah Anda?

Unity adalah nama desktop environment (user interface) resmi di OS Linux Ubuntu mulai versi desktop 11.04 hingga sekarang (15.04). Unity dinamakan Unity (Kesatuan) karena konsep Ubuntu yang sekarang mengarah kepada konvergensi (keseragaman, kesatuan ragam) karena Ubuntu tersedia di server, desktop, tablet, dan smartphone. Logo di samping adalah logo Unity.

Bagaimana Menggunakan Linux untuk Menangani Virus?

Tahu Solusi, Tahu Metodenya

Ade Malsasa Akbar <teknoloid@gmail.com>

Linux adalah hal yang asing bagi kebanyakan orang. Namun bagi komunitasnya, Linux sudah dikenal bagus untuk penanganan virus. Penanganan yang paling umum dilakukan adalah pencegahan. Linux diinstal di satu partisi tersendiri, digunakan ketika hendak memasukkan flash disk, setelah memeriksa pengguna restart ke Windows. Praktis, mudah. Penanganan jenis kedua adalah penyembuhan (**recovery**). Dengan teknologi LiveCD di Linux, Anda bisa memakai Linux dan seluruh programnya tanpa menginstal Linux ke hard disk. Mirip seperti menjalankan Windows tanpa menginstalnya. Dari Linux Live CD, Anda bisa memindai (scan) partisi Windows Anda dengan antivirus di Linux. Aman, efektif. Berikut kami berikan contoh-contoh penggunaan Linux untuk menangani virus.

LiveCD

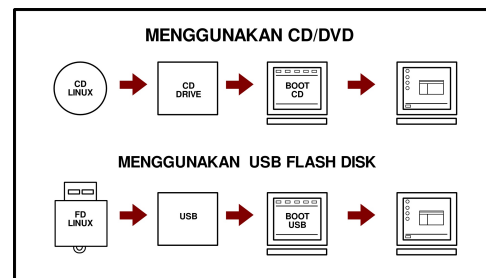



*Diagram **Booting** LiveCD Linux*

Contoh pertama adalah melakukan LiveCD Linux. Teknologi LiveCD membuat Linux bisa dijalankan dari CD tanpa diinstal ke hard disk. Windows tidak terganggu, partisi tidak terhapus, sistem tidak berat. Caranya adalah sediakan CD Linux (misalnya Ubuntu), masukkan ke cd drive, restart, atur **BIOS** supaya boot dari CD, lalu biarkan Linux dijalankan oleh komputer. Ini serasa menjalankan satu Windows sendiri. Lihat diagram di atas.

Dengan LiveCD, ada beberapa hal yang bisa Anda lakukan. **Pertama**, membuka (mount) partisi Windows. Ya, Linux bisa baca partisi Windows. **Kedua**, Anda bisa menghapus berkas. Penulis menggunakan cara ini untuk menghapus virus Yuyun.Cantik (virus shortcut **.lnk**) tanpa antivirus dan semua percobaan penulis sukses. Jika Anda tahu berkas berbahaya di partisi Windows, lebih aman menghapus dengan cara ini. **Ketiga**, Anda bisa menyalin (copy) berkas. Ini berguna ketika Anda tidak bisa login ke Windows. Anda bisa mem-**backup** data penting melalui Linux LiveCD ke HDD eksternal. **Keempat**, Anda bisa menimpa (replace) berkas. Hal ini berguna ketika ada berkas Windows (.dll misalnya) Anda yang korup. Dengan ini tampak gunanya Linux secara LiveCD.

Contoh Linux LiveCD (elementary OS)

Dualboot

Dualboot (boot ganda) adalah memiliki dua sistem operasi berbeda dalam satu komputer. Terdengar asing karena semua pengguna Windows menginstal 1 sistem operasi di 1 komputer. Tidak pernah lebih. Namun bagi pengguna Linux, dualboot adalah lumrah dan jamak. Jadi, Anda bisa menginstal Linux di partisi lain walaupun masih ada Windows di partisi lainnya. Tidak akan memberatkan komputer karena hanya 1 sistem yang berjalan dalam 1 waktu. Dan Anda bakal memilih login ke mana (ke Windows atau ke Linux) setiap restart. Lihat diagram berikut.

Dengan dualboot, ada beberapa manfaat layaknya LiveCD. **Pertama**, dualboot itu permanen. Maka Anda bisa menginstal antivirus di Linux, login ke Linux, dan scan partisi Windows secara teratur dari Linux. Dengan ini, Windows Anda aman. **Kedua**, Anda bisa memeriksa flash disk tanpa LiveCD. Karena repot jika harus LiveCD setiap ingin memeriksa flash disk. **Ketiga**, Anda bisa membantu orang. Restart ke Linux, buka flash disk-nya, hapus virusnya. Orangnya senang, komputer Anda tetap aman. **Keempat**, Anda bisa memeriksa seluruh partisi Windows tanpa login ke Windows. Lebih aman. Lebih terkendali.

Penutup

Apa yang tertulis dalam artikel ini adalah perkenalan. Pembaca didorong untuk belajar sendiri. Virus dan dampaknya, pencegahan dan solusinya, akan selalu menarik. Gunakanlah software yang legal, aman, dan bermanfaat.•

GLOSARIUM

Recovery
Operasi perbaikan sistem. Kadang digunakan untuk menyebut operasi pemulihan data yang terhapus. Recovery bisa dilakukan secara internal (dari dalam sistem) atau eksternal (dari luar sistem). Recovery dari dalam contohnya dengan antivirus.

Booting
Proses komputer menyala hingga sistem operasi berhasil dijalankan. Booting diatur oleh BIOS.

BIOS
Basic Input Output System. Program (firmware) di dalam mainboard yang mengatur booting sistem operasi.

.lnk
Dot EL EN KA (bukan II EN KA) adalah format untuk berkas desktop shortcut di Windows.

Backup
K Istilah untuk menyebut perbuatan atau hasil perbuatan backup. Pekerjaan mem-backup berarti menyalin data dari satu lokasi ke lokasi lain sebagai cadangan. Hasil backup juga disebut backup, yakni data cadangan dari data asli.

Codec
Compressor decompressor. Program yang mengodekan suara/gambar bergerak ke prosesor dan sebaliknya mengodekan balik data menjadi suara ke speaker.

Tahukah Anda?

Linux Mint adalah OS Linux turunan Ubuntu yang menyertakan **codec** (pemutar mp3 dsb.) yang tidak disertakan oleh Ubuntu. Linux Mint terkenal karena membuat desktop environment sendiri bernama Cinnamon yang elegan. Slogan Mint "*dari kebebasan muncul keanggunan*".

Tahukah Anda?

Satu hal menarik di dunia Linux adalah keamanan. Silakan pembaca mencari di internet "***pengguna linux 13 tahun tidak pernah kena virus***". Sebuah dialog menarik kisah pengguna Linux yang tidak pernah kena virus bertahun-tahun. Selain itu, ada juga artikel 10 tahun.

Tentang ROOTMAGZ

Majalah ini dibuat dengan free software (Scribus, Inkscape, Kate, KDE, Ubuntu). Majalah ini dibuat untuk memacu kontribusi masyarakat Indonesia dalam hal media massa digital untuk Linux. Semua ini dilakukan demi mengurangi pembajakan perangkat lunak di Indonesia. Tertanggal 12 September 2015

Kontak Redaksi
Ade Malsasa Akbar
desaininkscape.wordpress.com
teknoloid@gmail.com

Spesifikasi Majalah
Fonta: FreeSans, Droid Sans
Fonta Logo: Bitsumishi
Dimensi: A4 Landscape
Ikon: KDE Oxygen, Faenza, Wikipedia.org
Cover background: unsplash.com (PD)

Lisensi